ANALISIS KESELAMATAN RANGKAIAN TANPA WAYAR DI KOLEJ PENDETA ZA'BA

IDZA AISARA BINTI NORABID
DR. ROSSILAWATI SULAIMAN

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

WIFI ialah singkatan kepada wireless fidelity merupakan sesuatu teknologi penghantaran tanpa wayar julat dekat untuk mengakses Internet dalam konteks isyarat radio. Walaupun teknologi rangkaian tanpa wayar ini mempunyai banyak kebaikan tetapi rangkaian ini lebih mudah terdedah kepada serangan kerana ketidakcukupan penggunaan perlindungan mekanisme rangkaian tanpa wayar. Oleh itu, kajian ini bertujuan untuk membantu pengguna menubuhkan platform rangkaian aplikasi yang teguh untuk rangkaian tanpa wayar. Dengan menggunakan sistem operasi Kali Linux, sebuah perisian sumber terbuka, beberapa pengujian terhadap rangkaian tanpa wayar yang terlibat telah dijalankan. Hasil pengujian yang telah dilakukan telah direkodkan dan dianalisa agar dapat dijadikan panduan untuk masa hadapan.

1. PENYATAAN MASALAH

Walaupun teknologi rangkaian tanpa wayar ini mempunyai banyak kebaikan tetapi rangkaian tanpa wayar ini lebih mudah terdedah kepada serangan kerana keselamatan rangkaian tanpa wayar ini sangat rendah jika dibandingkan dengan keselamatan wayar kabel internet dan ia kekal menjadi risiko keselamatan yang tinggi untuk rangkaian tempatan.

Hal ini terutamanya berlaku disebabkan oleh medium komunikasi iaitu udara, yang boleh dicapai dalam linkungan tindakan yang spesifik. Selain itu, ketidakcukupan penggunaan perlindungan mekanisme rangkaian tanpa wayar turut menjadi faktor rangkaian ini lebih terdedah kepada risiko (Skendzic & Kovacic 2014). Kajian ini menyedarkan pihak pengguna tentang keteguhan keselamatan sesebuah rangkaian. Oleh itu, sangat penting untuk pengguna mengetahui tentang langkah keselamatan yang sesuai untuk rangkaian wayar ini, bagi memastikan keteguhan sesebuah operasi walaupun dalam kes serangan hasad.

2. OBJEKTIF KAJIAN

i. Menganalisis faktor yang melibatkan keselamatan penggunaan rangkaian tanpa wayar
ii. Mengumpulkan data yang diperoleh daripada artikel , jurnal dan lain-lain
iii. Menjalankan beberapa pengujian ke atas rangkaian tanpa wayar

3. METODOLOGI

Metod yang digunakan untuk kajian ini ialah dengan melaksanakan fasa-fasa yang dinyatakan seperti berikut.

4.1 FASA KAJIAN KESUSASTERAAN

Fasa ini memainkan peranan yang penting untuk membolehkan pengujian berjalan dengan sempurna. Pencarian pelbagai maklumat meliputi pengujian rangkaian dan perisian serta kajian kesusateraan sebagai maklumat sokongan. Sebagai contoh, kriteria ketakteguhan rangkaian tanpa wayar telah diperoleh melalui analisis artikel yang berkait.

4.2 FASA ANALISIS KEPERLUAN

Fasa ini merangkumi pencarian maklumat yang berkaitan dengan perisian yang bakal digunakan dalam kajian ini. Ciri-ciri perisian terbabit diselidiki agar mudah untuk menggunakannya semasa dalam fasa implementasi.

Tujuan analisis ini dilakukan adalah :

I. untuk mendapatkan maklumat tentang perisian sedia ada

II. untuk mendalami fungsi perisian yang terpilih

4.2.1 KEPERLUAN PERISIAN

Keperluan perisian merangkumi bahagian yang tidak kelihatan di dalam sistem. Perisian yang digunakan untuk menguji rangkaian ialah sistem pengoperasian Kali Linux.

4.2.2 KEPERLUAN PERKAKASAN

Keperluan perkakasan merangkumi bahagian yang kelihatan dan boleh disentuh oleh pengguna. Bahagian inilah yang menghubungkan antara pengguna dan sistem. Perkakasan yang diperlukan ialah kelajuan pemproses 2.3Ghz , Memori Capaian Rawak (RAM) 4Gb dan penyesuai rangkaian 802.11.

4.3 FASA IMPLEMENTASI

Fasa ini merupakan fasa kritikal dimana ia mengetengahkan pelaksanaan pengujian rangkaian berdasarkan hasil kajian daripada fasa yang sebelum. Fasa ini dilakukan dengan membangunkan makmal pengujian rangkaian secara maya dan menjalankan pengujian rangkaian yang tertumpu di Kolej Pendeta Za'ba.

4.4 FASA ANALISIS

Fasa ini merupakan fasa menganalisis hasil dapatan kajian dan juga menyediakan laporan berdasarkan hasil yang telah didapati.

5. HASIL KAJIAN

5.1 PENGENALAN

Kali-Linux merupakan sebuah sistem operasi keluaran Linux ditujukan untuk pengujian penembusan maju dan pemeriksaan keselamatan. Sistem operasi ini mengandungi ratusan alat pengujian yang ditujukan kepada pelbagai tugas yang melibatkan keselamatan maklumat seperti Pengujian Penembusan, Penyelidikan Keselamatan, Forensik Komputer dan Kejuruteraan Balikan.

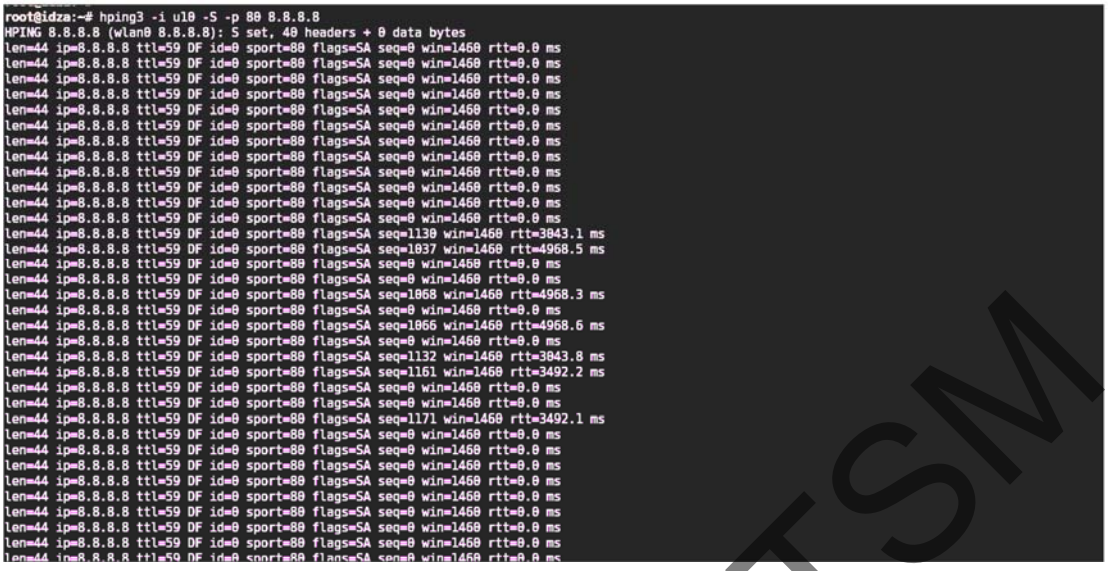
5.2 DOS ATTACK TERHADAP HALAMAN LOG MASUK UKM WIFI

Rajah 1 : Perintah 'nslookup'

Seperti laman sesawang yang lain, halaman log masuk mempunyai IP Address yang tersendiri yang membolehkan maklumat daripada server dipaparkan kepada pengguna. Perintah 'nslookup' dapat memberikan maklumat tentang IP Address yang dikehendaki. Rajah 1 menunjukkan IP Address untuk halaman log masuk UKM WIFI.

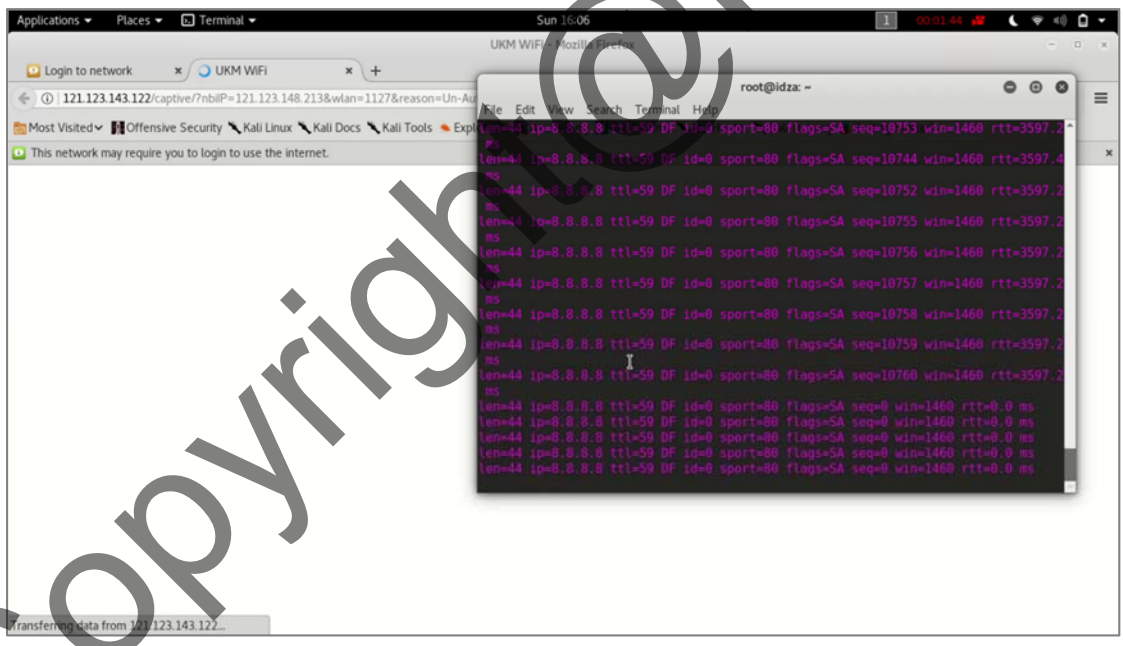
Sekiranya permintaan untuk mengakses sesebuah laman sesawang itu tinggi, maka hal ini boleh melambatkan atau memberhentikan akses kepada sesebuah laman sesawang. Kedua perkara tersebut merupakan objektif utama kepada serangan DOS (denial of service) ini. Siri serangan DOS ini telah dijalankan dengan menggunakan perisian hping. Menurut rajah 2, perintah 'hping -i u10 –S –p 80 8.8.8.8' telah digunakan dimana –i mewakili jeda masa (uX wakili X mickrosaat) , –S untuk menetapkan bendera SYN, -p merujuk kepada port destinasi dan yang terakhir destinasi IP Address.

Merujuk rajah 3, halaman log masuk tidak dapat diakses dalam tempoh 1:30 minit semasa serangan sedang dijalankan berbanding dengan tempoh 5 saat apabila serangan tidak dijalankan.



Rajah 2 : Serangan DOS sedang dijalankan

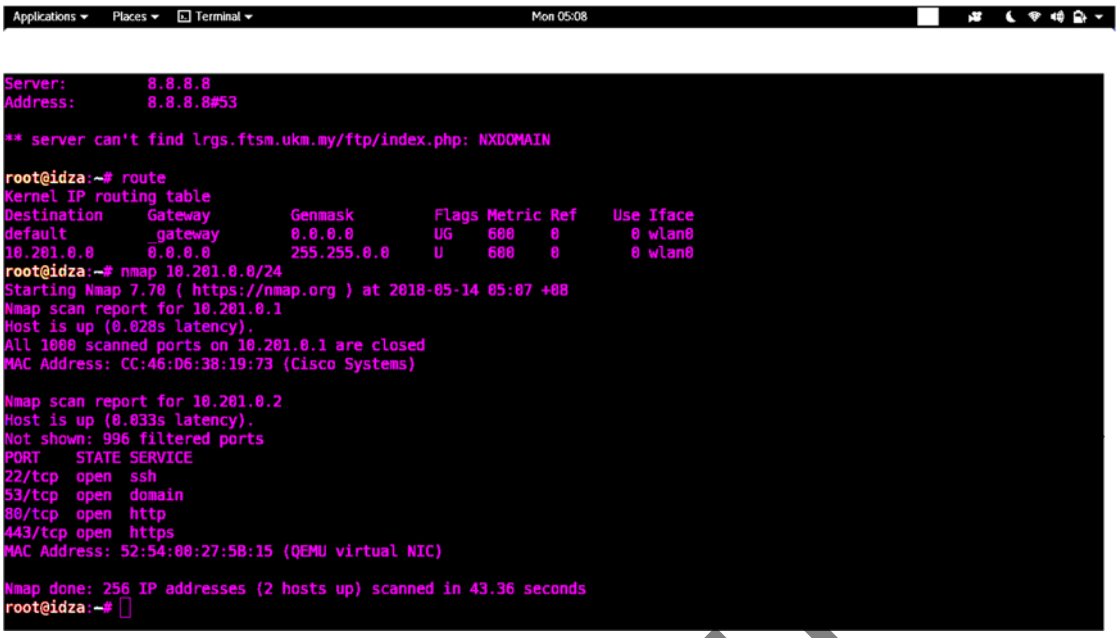
#



Rajah 3 : Halaman log masuk semasa serangan DOS sedang dijalankan

5.3 SERANGAN MAN-IN-THE-MIDDLE

Man-in-the-middle adalah salah satu bentuk serangan yang membolehkan penyerang mendapatkan maklumat daripada pihak mangsa tanpa disedari. Serangan ini dilakukan ke atas rangkaian dengan hanya mengenalpasti IP Address mangsa dan default gateway rangkaian tersebut.



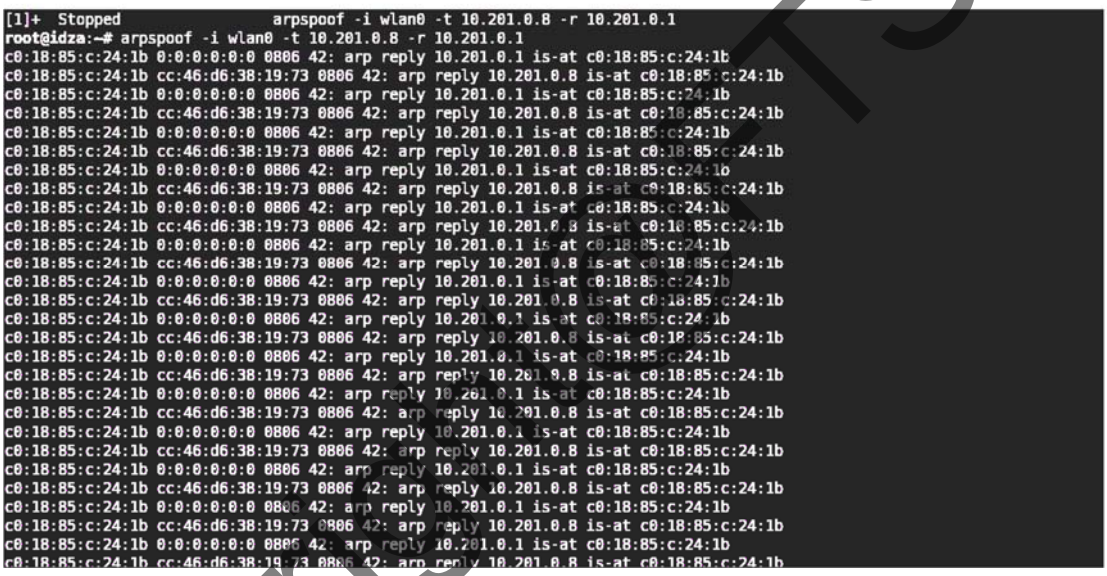
Rajah 4 : Perintah 'route' dan 'nmap'

Perintah 'route' akan memaparkan jadual penghalaa IP dan dijalankan bagi mengetahui default gateway dan 'nmap' akan memaparkan hos dan khidmat dalam sesebuah rangkaian komputer. Perisian Ettercap pula dapat memaparkan senarai pengguna yang berada di dalam lingkungan subnet yang sama.

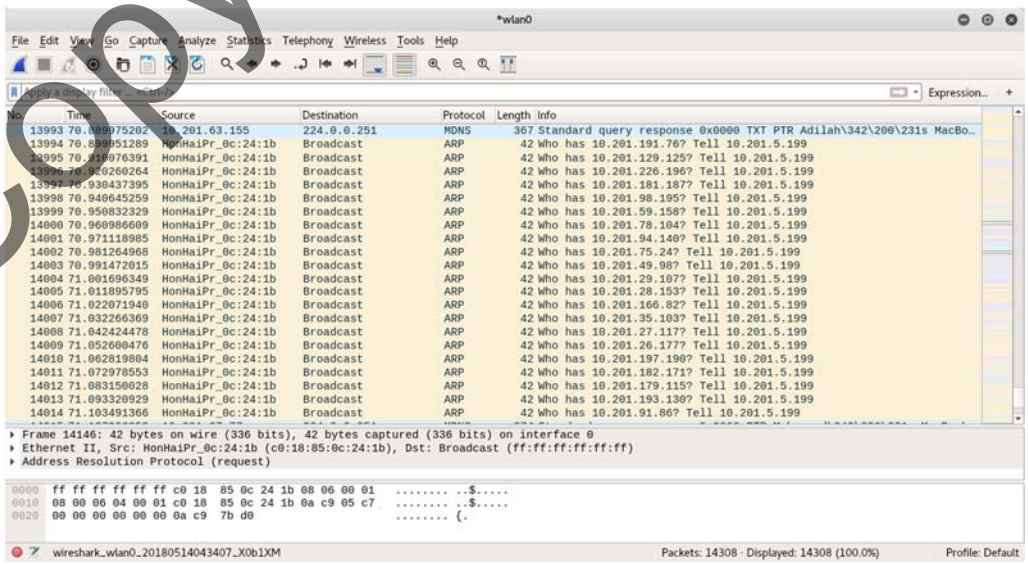
Rajah 5 : Senarai *IP Address* mangsa

Setelah IP Address mangsa dan default gateway telah dikenal pasti, perintah ‘arpspoof –i wlan0 –t 10.201.0.8 –r 10.201.0.2 ‘ dimana –i merujuk kepada antara muka tanpa wayar , -t mewakili IP Address mangsa dan –r mewakili default gateway.

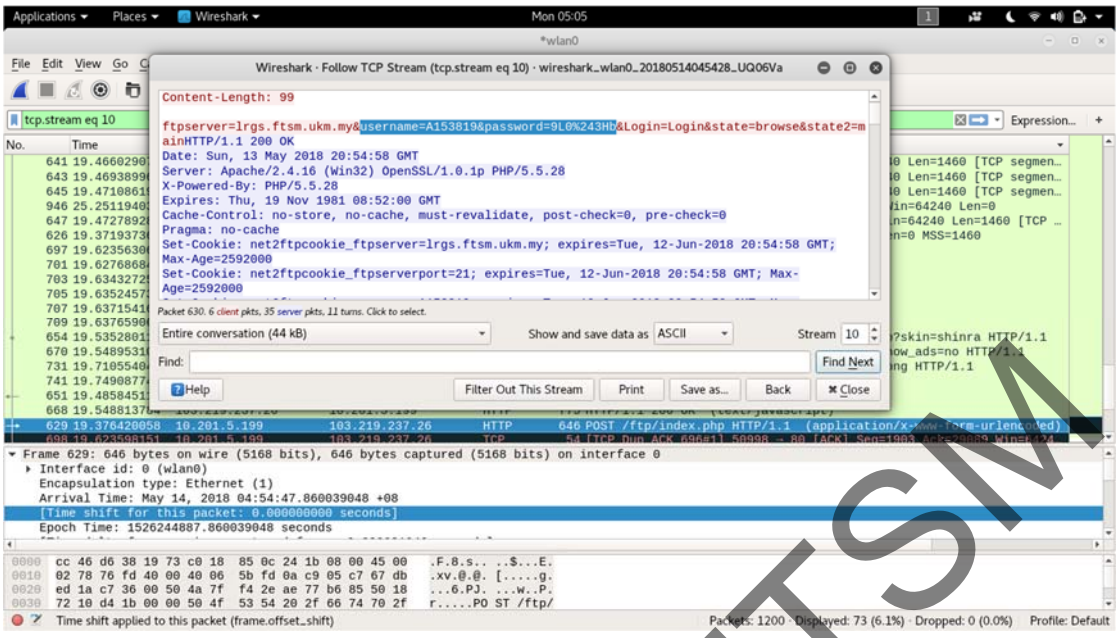
Dalam rajah 7, aliran trafik mangsa dipantau menggunakan perisian Wireshark. Risiko ini sangat tinggi apabila mangsa melayari laman sesawang yang mempunyai keselamatan yang rendah seperti laman sesawang yang bukan dilabel https. Seperti yang terdapat di rajah 8, penyerang boleh melihat username dan password mangsa secara terangan.



Rajah 6 : *Address Resolution Protocol (ARP) spoof*



Rajah 7 : Aliran trafik semasa arpspoof dijalankan



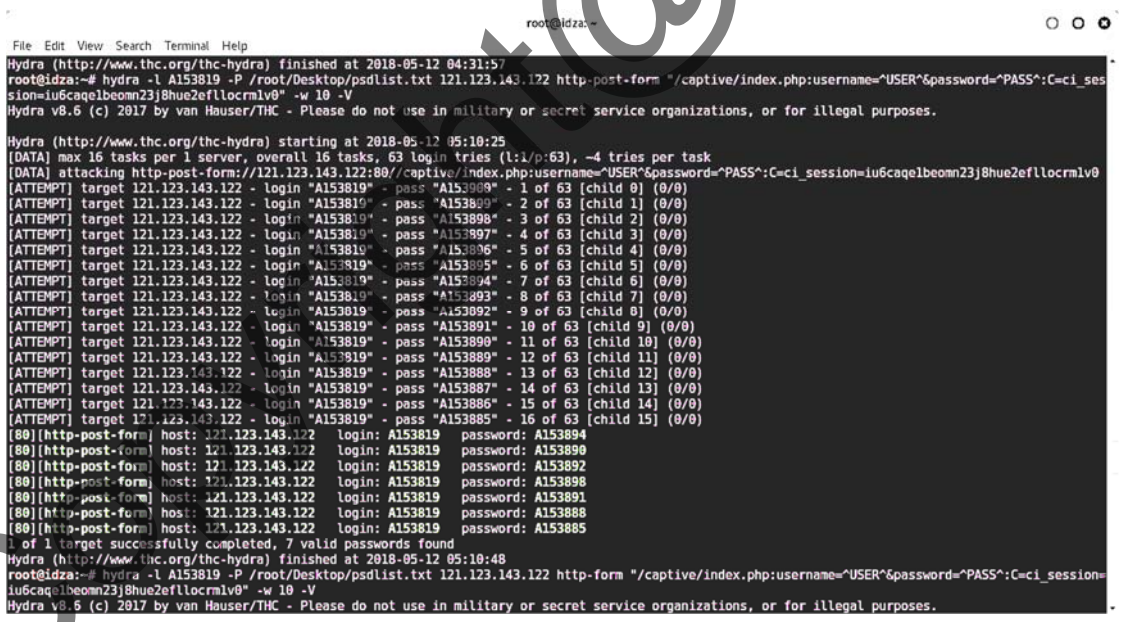
Rajah 8 : *Username* dan *password* yang dapat dihidu Wireshark

5.4 BRUTE FORCE ATTACK TERHADAP HALAMAN LOG MASUK

Rangkaian tanpa wayar UKM WIFI mempunyai log masuk yang berhubung dengan pangkalan data untuk mengesahkan penggunaannya. Pangkalan data yang menyimpan maklumat sulit halaman log masuk (seperti username dan password) boleh diceroboh sekiranya penyerang tahu segala kebarangkalian maklumat yang boleh digunakan. Rajah 9 menunjukkan kata laluan yang boleh dijadikan panduan untuk proses pencarian kata laluan mangsa di halaman log masuk UKM WIFI.

Kemudian, perisian Hydra digunakan bagi melaksanakan brute force terhadap halaman masuk UKM WIFI melalui kombinasi yang sepadan. Perintah ‘hydra -l A153819 -P /root/Desktop/psdlist.txt 121.123.143.122 http-get-form "/captive/index.php:username=^USER^&password=^PASS^:C=ci_session=iu6caqe1beomn23j8hue2efllocrm1v0" -w 10 –V’ telah digunakan dimana –l mewakili username -P senarai kata laluan diikuti dengan destinasi folder , IP Address laman tersebut, jenis GET/POST , index,php yang mewakili destinasi setelah laman dimasuki data, ^USER^&^PASS^ bagi Hydra mencuba senarai user atau password yang telah disediakan. Dengan data yang telah dberikan, akhirnya, kata laluan pelajar ditemui. Namun begitu, di dalam kajian ini, hasilnya merupakan hasil ‘false positive’ kerana kata laluan yang berjaya ditemui tidak begitu tepat.

Rajah 9 : Senarai kata laluan yang dijadikan panduan



Rajah 10 : Kata laluan yang ditemui

#

6. KESIMPULAN

Secara kesimpulannya, didapati bahawa keselamatan rangkaian yang telah dilakukan pengujian ke atas nya mempunyai keselamatan yang rendah kerana beberapa serangan berjaya dilakukan. Serangan-serangan ini dapat dielakkan jika dikesan terlebih dahulu dan dapat mengimplimentasikan kaedah yang bersesuaian untuk mencegah serangan tersebut. Namun begitu, segala keteguhan keselamatan rangkaian ini harus dipuji dan perlu dikekalkan prestasi yang baik itu. Selain itu, kelebihan dan kekurangan kajian ini dinyatakan agar boleh dijadikan iktibar kepada pengguna laporan ini.

7. RUJUKAN

Abdelrahman, A. A., Fouad, M. M. & Dahshan, H. M. 2017. Analysis on the AES implementation with various granularities on different GPU architectures. *Advances in Electrical and Electronic Engineering*, *15*(3), 526–535. doi:10.15598/aeee.v15i3.2324

Bhatnagar, R. & Kumar Birla, V. 2015. Wi-Fi Security: a Literature Review of Security in Wireless Network. *International Journal of Research in Engineering & Technology*, *3*(5), 2321–8843.

Carlson, J. & Levkowetz, H. 2004. Extensible Authentication Protocol (EAP) 1–67.

Chhillar, R. S. 2012. Review of WI-FI Security techniques *2*, 3479–3481.

Fips, N. 2001. 197: Announcing the advanced encryption standard (AES). … *Technology Laboratory, National Institute of Standards …*, *2009*, 8–12. doi:10.1016/S1353-4858(10)70006-4

Gopalakrishnan, S. 2014. a Survey of Wireless Network Security *3*(1), 53–68.

Han, W., Zheng, D. & Chen, K. F. 2009. Some remarks on the TKIP key mixing function of IEEE 802.11i. *Journal of Shanghai Jiaotong University (Science)*, *14 E*(1), 81–85. doi:10.1007/s12204-009-0081-8

Kelsey, J., Schneier, B. & Wagner, D. 1996. Key-Schedule Cryptanalysis of {IDEA}, {G-DES}, {GOST}, {SAFER}, and Triple-{DES}. *Advances in Cryptology---CRYPTO~'96*, 237–251. doi:10.1007/3-540-68697-5_19

Lane, H. 2012. Interested in learning SANS Institute InfoSec Reading Room Wireless LAN Technology In tu f rig. *Technology*,.

Micol, 2012. Temporal Key Integrity Protocol (TKIP). https://www.slideserve.com/micol/temporal-key-integrity-protocol-tkip [10 Disember 2017].

Packt, 2016. Common WLAN Protection Mechanisms and their Flaws. https://hub.packtpub.com/common-wlan-protection-mechanisms-and-their-flaws/ [10

Disember 2017].

Peng, H. 2012. WIFI network information security analysis research. *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, 21-23 April*, 2243–2245. doi:10.1109/CECNet.2012.6201786

Rubin, A. D. 2003. Wireless Networking Security. *Association for Computing Machinery. Communications of the ACM*, *46*(5), 28–30. doi:http://dx.doi.org/10.1145/769800.769821

Skendzic, A. & Kovacic, B. 2014. Security analysis of wireless network access following 802.11 standard in educational institutions of the Republic of Croatia. *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, (May), 929–936. doi:10.1109/MIPRO.2014.6859701

To, A. G. & Network, W. 2004. Still Secure ® (July).

Zou, Y., Zhu, J., Wang, X. & Hanzo, L. 2016. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, *104*(9), 1727–1765. doi:10.1109/JPROC.2016.2558521